

ADMINISTRACIÓN Y GESTIÓN DE SERVICIOS DE INFRAESTRUCTURA EN ZETYL

César Fernando Espitia Pérez, Cristóbal García Viviescas, Oscar Andrés Díaz Novoa, Brayan Alexis López Chaves
Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI, Universidad Nacional Abierta y a Distancia UNAD
Bogotá, Colombia

espitiap.cesarf@gmail.com
cristobal.garcia.viviescas@gmail.com
Oscarsanti2@yahoo.com.ar
brayanlopez8@gmail.com

Resumen

En el avance de la sociedad actual no es extraño que desde las primeras etapas del desarrollo de los seres humanos están influenciados por la tecnología, a tal punto que se ha hecho primordial aprender y hacer uso de la misma en la cotidianidad; con cada avance se abren diferentes opciones para pensar y reflexionar sobre el manejo y uso de la información y la comunicación, además de la importancia de la seguridad en el campo tecnológico. La seguridad informática no sólo atañe a los individuos, sino a empresas o compañías que requieren un manejo adecuado y restringido de su información, los cuales pueden estar en riesgo cuando se utiliza una red, por lo cual se crean usuarios dentro de una organización, de tal forma, que allí cobra relevancia Zentyal como una herramienta de protección de una red de datos que facilita el manejo de y la administración de la información en una compañía.

A lo largo de este artículo se encuentra la consolidación para debatir, generar, determinar e implementar soluciones GNU/Linux, a través del uso de la herramienta llamada Zentyal Server, como mecanismo de seguridad y gestión a partir de este Sistema Operativo robusto y fácil de administrar al interior de una compañía. Zentyal Server de linux nos ofrece una solución para administrar servicios como DHCP, DNS, Active Directory entre otros muchos servicios, fácil de administrar e instalar, muy similares a los ofrecidos por Microsoft Windows Server, Zentyal se enfoca principalmente para las pequeñas empresas y es una alternativa para Windows Small Bussines Server la cual tiene costos de licenciamiento.

Palabras claves:

Dominio, DHCP, Proxy no transparente, Cortafuegos o firewall, Seguridad informática.

Abstract—

In the advance of current society it is not strange that from the first stages of the development of human beings are influenced by technology, to the point that it has become essential to learn and make use of it in everyday life; With each advance, different options are opened to think and reflect on the management and use of information and communication, as well as the importance of security in the technological field. Computer security not only concerns individuals, but companies or companies that require adequate and restricted management of their information, which may be at risk when a network is used, for which users are created within an organization, such form, that Zentyal becomes relevant as a protection tool for a data network that enters interacting in a company.

Throughout this article is the consolidation of debating, generating, determining and implementing GNU / Linux solutions, through the use of the tool called Zentyal Server, as a security and management mechanism based on this robust and easy operating system manage. Zentyal Server of Linux offers us a solution to manage services such as DHCP, DNS, Active Directory among many other services, easy to administer and install, very similar to those offered by Microsoft Windows

Server, Zentyal focuses mainly for small businesses and is a alternative for Windows Small Bussines Server which has licensing costs

Keywords:

Domain, DHCP, Non-transparent proxy, Firewall , Computer security

I. INTRODUCCIÓN

Los ingenieros de sistemas están expuestos a responder a los retos y desafíos que a diario se plantean como fruto de los nuevos desarrollos científicos, tecnológicos e informáticos que parecieran ser más acelerados que las propias respuestas que se puedan dar en un instante, pero que al final es necesario dar soluciones efectivas que favorezcan una mejor calidad de vida y de funcionamiento estratégico de las diferentes instituciones, entidades y compañías públicas o privadas.

Estas soluciones son necesarias en todos los ámbitos del desarrollo de la sociedad, para este se identificó la necesidad de la seguridad informática en una compañía y la accesibilidad para los usuarios, para este caso tomará las herramientas de seguridad Zentyal como estrategia para la seguridad de una compañía, la cual nos proveerá un plus de herramientas para la seguridad de nuestra red de datos, en donde se utilizar servidor.

II. MARCO TEÓRICO

A continuación, se plantean los referentes conceptuales esenciales para la comprensión de la presente investigación,

- 1) **Sistema Operativo:** (SO o, frecuentemente, OS —del inglés operating system—) es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes (aunque puede que parte de él se ejecute en espacio de usuario) (Linode, s.f; a)
- 2) **Gnu/Linux:** también conocido como Linux, es un sistema operativo libre tipo Unix;

multiplataforma, multi-usuario y multi-tarea. El sistema es la combinación de varios proyectos, entre los cuales destacan GNU (encabezado por Richard Stallman y la Free Software Foundation) y el núcleo Linux (encabezado por Linus Torvalds). Su desarrollo es uno de los ejemplos más prominentes de software libre: todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera, bajo los términos de la GPL (Licencia Pública General de GNU) y otra serie de licencias libres. (Linode, s.f, b)

- 3) **Zentyal Server 5:** se basa en Ubuntu 16.04, una versión autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios (Pedraza, et al, s.f.)

LTS de Canonical que no sólo contiene la última versión estable del kernel sino que también tiene un soporte para empresas excepcional. Sin olvidar que contiene dos actualizaciones y próximamente se lanzará una versión de actualización que modernizará el sistema, no sólo de Ubuntu sino de las distribuciones que se basen en ello, como en este caso Zentyal compartidas. Actualmente existen servidores de impresora para interfaz paralela, USB o impresoras de red.

- 4) **Vpn:** red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre Linux con sencillez de implementación (Delgado, 2014)
- 5) **Proxy:** Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza

un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina **A** solicita un recurso a **C**, lo hará mediante una petición a **B**, que a su vez trasladará la petición a **C**; de esta forma **C** no sabrá que la petición procedió originalmente de **A**. (Delgado, 2014).

- 6) **Firewall:** Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. (Nuami, s.f)
- 7) **Dhcp:** Es un servidor que usa protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Así los clientes de una red IP pueden conseguir sus parámetros de configuración automáticamente (Suarez, 2016a)
- 8) **Dns:** El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente (Suarez, 2016b)
- 9) **Print Server:** Es un concentrador, o más bien un servidor, que conecta una impresora a red, para que cualquier PC pueda acceder a ella e imprimir trabajos, sin depender de otro PC.

Zentyal se distribuye en dos paquetes:



Zentyal Server para PYMEs y Zentyal Cloud para proveedores de hosting. Zentyal Server tiene una edición de desarrollo que puede descargarse de forma gratuita y cuyo código fuente está disponible bajo los términos de la GNU General Public License.

ZENTYAL SERVER 5.0

Zentyal es una solución de correo electrónico y groupware de código abierto, compatible de forma nativa con Microsoft Outlook. Zentyal implementa protocolos Microsoft Exchange sobre componentes estándares de código abierto (como Dovecot, Postfix, Samba, etc.) para proporcionar compatibilidad nativa con clientes Microsoft Outlook. Los protocolos de correo electrónico y groupware soportados por Zentyal son MAPI, ActiveSync, EWS, SMTP, POP, IMAP, CalDAV, CardDAV y Active Directory (Zentyal, s.f.)

Zentyal se distribuye en dos paquetes: Zentyal Server para PYMEs y Zentyal Cloud para proveedores de hosting. Zentyal Server tiene una edición de desarrollo que puede descargarse de forma gratuita y cuyo código fuente está disponible bajo los términos de la GNU General Public License.

Zentyal está constituida como la primera implementación nativa del conocido Directorio Activo de Microsoft en ambientes

C. Firewall Zentyal

El Firewall de Zentyal está basado en el framework Netfilter que viene incluido en el kernel de GNU/Linux desde la versión 2.4.x. Y la gestión de este a través del panel de administración web es bastante sencilla, ya

<https://doc.zentyal.org/es/firewall.html>

La administración del Firewall en Zentyal está organizada en 4 subgrupos a saber:

- ### E. Objetos de red

El concepto de *Objeto de Red* es una forma que maneja Zentyal para poder realizar tareas de gestión y administración sobre grupos de elementos de red identificándolos principalmente por sus direcciones IP y/o sus MAC. Simplificando la tarea de aplicar sobre ellos reglas de restricción o acceso a diferentes redes o recursos de red específicos (Zentyal, s.f).

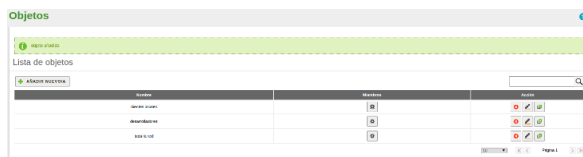


Fig. 2 Objetos de red en Zentyal (<https://doc.zentyal.org/es/abstractions.html#gestion-de-los-obietos-de-red-con-zentyal>)

PERFIL DE ZENTYAL	USUARIOS	CPU	MEMORIA	DISCO	TARJETAS DE RED
Puerta de acceso	<50	P4 o superior	2G	80G	2 ó más
	50 ó más	Xeon Dual core o superior	4G	160G	2 ó más
Infraestructura	<50	P4 o superior	1G	80G	1
	50 ó más	P4 o superior	2G	160G	1
Oficina	<50	P4 o superior	1G	250G	1
	50 ó más	Xeon Dual core o superior	2G	500G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Depende de un proveedor de internet donde se comparte el canal y se tienen diferentes velocidades de subida y bajada se puede presentar lentitud, también dificultades si no se tiene una infraestructura adecuada en el servidor.

Fig. 3 Requerimientos hardware para uso de Zentyal

I. TEMATICA 1: DHCP SERVER, DNS SERVER Y CONTROLADOR DE DOMINIO.

El servidor Zentyal nos permite administrar nuestra red de una forma sencilla y de forma modular seleccionando la opción Network configuration.

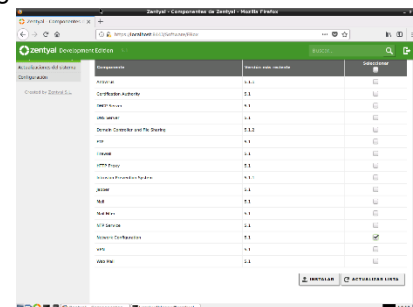


Fig. 4 Instalación componente network Configuration

Configuración de las interfaces, en este caso verificar por medio de RED Interna cual es la IP

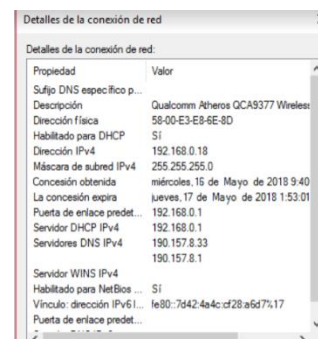


Fig. 5 Verificación estado de red



Fig. 6 Configuración de tipos de interfaces

Selección de método, dirección IP y máscara de red Se configura las interfaces de red, Eth0= adaptador de internet, con DHCP y WAN, Eth1- adaptador puente, Con static y es ingresa la IP

Fig. 7 Configuración de red para interfaces externas

Se verifica que la configuración este de acuerdo con los parámetros establecidos.



Fig. 8 Verificación configuración.

Se realiza ping para validar la correcta conectividad

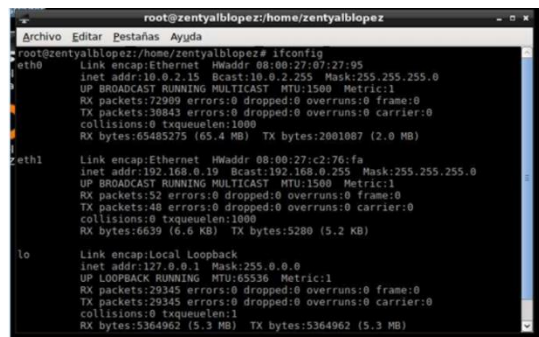


Fig. 9 Detalle de Red

Configuración de DHCP y DNS en Zentyal
DHCP: Dynamic Host Control Protocol o Protocolo de Control Dinámico de Host.

Con este protocolo un host nuevo puede resolver una petición para obtener información IP. El servidor DHCP proporciona al host toda

la información necesaria para comunicarse en la red, como su dirección IP, la máscara de red, la puerta de enlace, los servidores DNS a utilizar y una serie de parámetros que dependiendo de la necesidad se podrían configurar. Sin el uso de este servidor tendríamos que poner toda la información manualmente en cada dispositivo, y si el dispositivo se mueve a otra subred, se debe configurar otra dirección IP diferente.

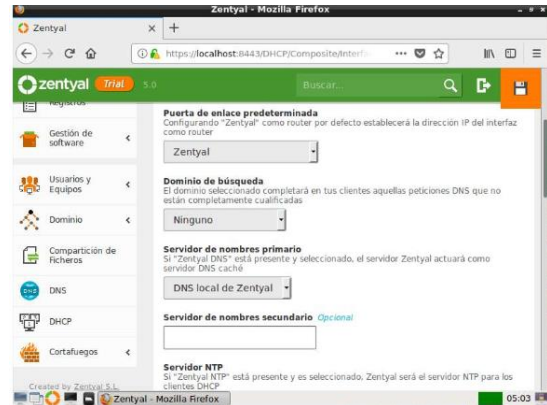


Fig. 9 Otras configuraciones necesarias

El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias, y automáticamente asignar y enviar si fuera el caso, una nueva IP al dispositivo si se conectase en un lugar diferente de la red.

El servidor DHCP debe trabajar junto al servidor DNS para crear el sistema de DNS dinámico, por lo que se ha de tener en cuenta para la configuración adecuada.

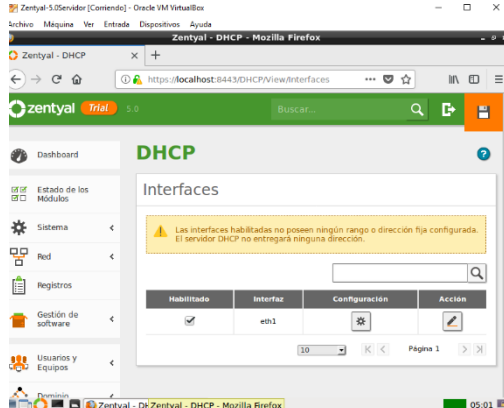


Fig. 10 Configuración de red para interfaces externas

La configuración de DNS es vital para el funcionamiento de la autenticación en redes locales (implementada con Kerberos a partir

de Zentyal 3.0), los clientes de la red consultan el dominio local, sus registros SRV y TXT para encontrar los servidores de tickets de autenticación

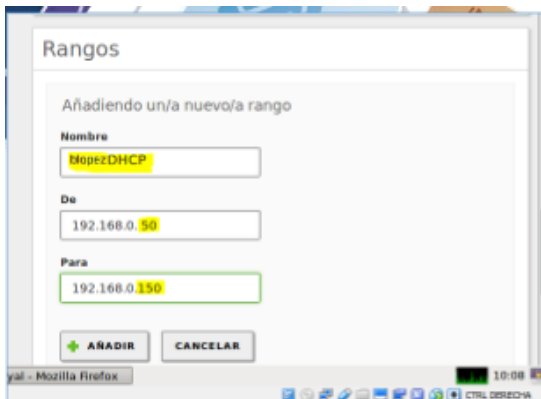


Fig. 11 Rangos permitidos y subnet

Si se requiere adicionar un nuevo dominio se agrega en este caso se realizará solo con el dominio local.

Se configuran el módulo de DHCP, Se verifica las conexiones de red activa, se realiza un ping para la verificación y estado de la red.

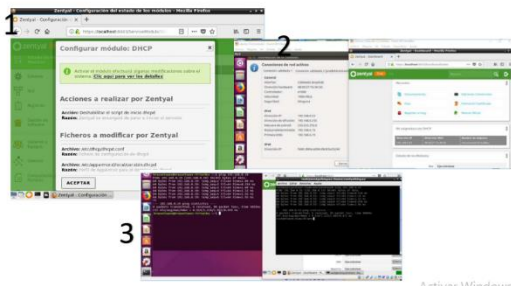


Fig. 12 Pasos de Configuración DHCP.

Se agrega un nuevo dominio, verificación de estado de los módulos, se realiza una verificación del estado de la red.



Fig. 13 Pasos de configuración de servidor de Dominio.

Control de dominio

Se ingresa a la pantalla de dominio, se asigna un nombre de dominio, nombre de máquina, se asigna una letra a la unidad, se agregan los usuarios y los equipos, se realiza la configuración de contrafuegos.

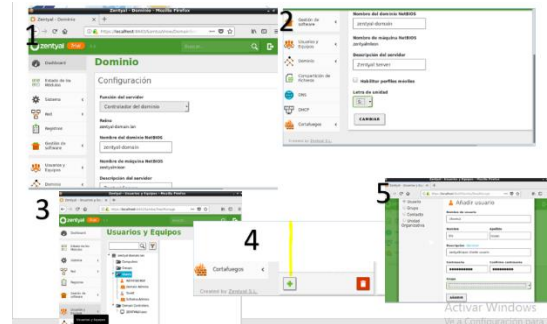


Fig. 14 Ajustes de dominio necesarios.

Se crean usuarios o grupos según la necesidad de negocio y el tamaño del entorno en el que se aplicara, se realiza las validaciones necesarias para verificar la correcta configuración.

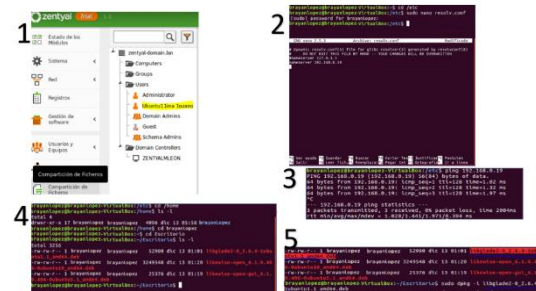


Fig. 15 Pasos para la inclusión de usuarios de dominio

Se une al directorio activo cada uno de los usuarios.

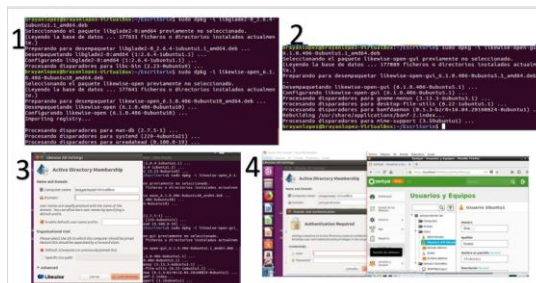


Fig. 16 pasos de verificación de dominio usuarios y equipos

Domain Join Authentication

 **Authentication Required**

Joining a machine to Active Directory requires credentials for a Windows user with administrative privileges in the target domain.

Credentials

User:

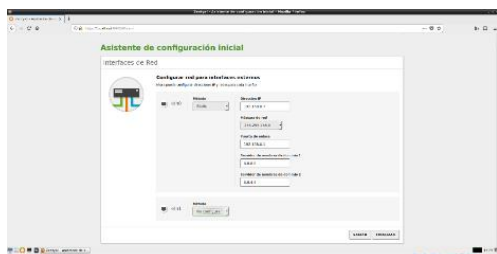
Password:

TEMÁTICA	2:	PROXY	NO
TRANSPARENTE			

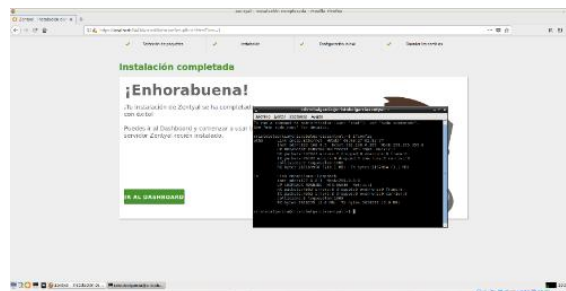
Instalación de aplicación

-

b) Configuración de red de datos, el cual tiene objetivo de realizar la conexión de puerta de enlace para la salida hacia internet y determinar las posibles restricciones que se puedan configurar.



Con el anterior instructivo se tendrá la instalación del Proxy dentro de Zentyal, lo cual permite que se realicen la configuración deseada dentro de Zentyal para contralara el tráfico sobre la red y así empezar a garantizar la seguridad dentro de nuestra red de datos.



Configuración Proxy en Zentyal

The screenshot shows the AWS IAM console dashboard. The top navigation bar includes the AWS logo, the text 'IAM', and a search bar. The main content area is titled 'Dashboard' and displays the 'root' user's details, including their email address, MFA status, and a list of IAM roles. The 'root' user is shown as having no MFA device and being able to use the console. The 'IAM roles' section lists several roles, including 'AWS_IAM_ROLE_FOR_EC2_INSTANCE_PROFILE', 'AWS_IAM_ROLE_FOR_EC2_INSTANCE_PROFILE', 'AWS_IAM_ROLE_FOR_EC2_INSTANCE_PROFILE', 'AWS_IAM_ROLE_FOR_EC2_INSTANCE_PROFILE', and 'AWS_IAM_ROLE_FOR_EC2_INSTANCE_PROFILE'. The 'root' user is also shown as having no MFA device and being able to use the console.

a) Verificación de la configuración de red y ajustes, en esta se valida las entradas en las tarjetas de red eth0 y eth1, en donde se deja por defecto la eth0 y la eth1 debe quedar como DHCP para que esta lleve la salida hacia la Wan, posteriormente se verifica el puerto de conexión del Proxy el

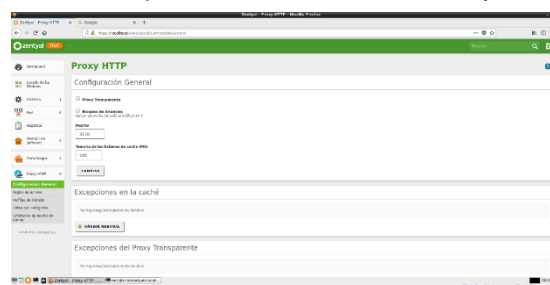


Fig. 22 Verificación de puesto de conexión en Zentval

- b) Acciones de verificación de configuración sobre el funcionamiento del proxy, después de realizar las configuraciones antes mencionadas se ingresa a un cliente Linux o Windows en donde se direcciona al navegador web por defecto establecido en el cual se incluye el Proxy configurado para nuestro caso 192.168.0.7. y valida la navegación.

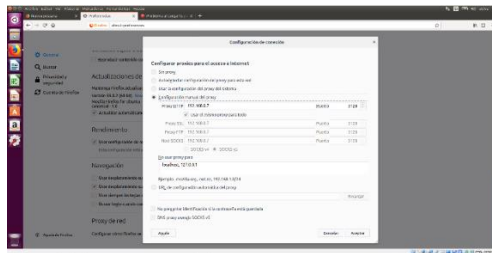


Fig. 23 Ingreso de datos de Proxy

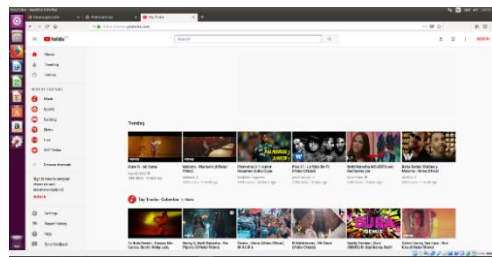


Fig. 24 Navegación de Proxy

c) **Personalización de Zentyal.**

Después de la configuración e instalación de Proxy, es posible la personalización del mismo a través de perfiles de filtrado, en donde es posible crear reglas, las cuales se le asignaran al o los perfiles para su mayor control y protección a red.

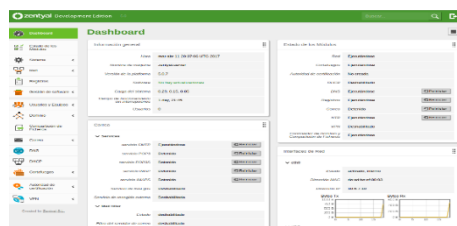


Fig. 25 Perfiles de filtrado zentyal

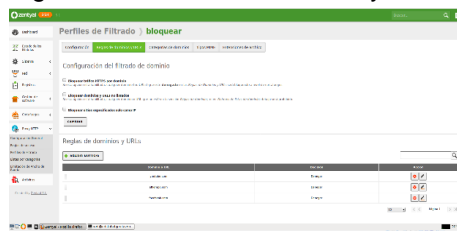


Fig. 26 Regla de acceso zentyal

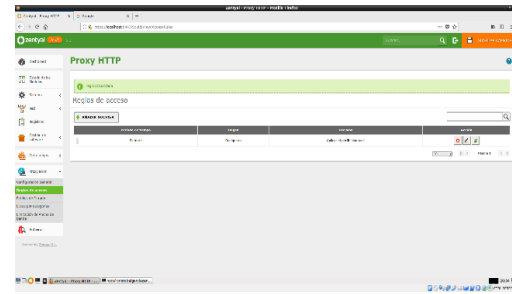


Fig. 27 Asignación de Regla de acceso zentyal

Validando la configuración antes mencionada se lograr crear una regla de acceso más limitado en el Proxy bloqueando diferentes páginas, para así lograr una filtrado dentro de la red de datos.

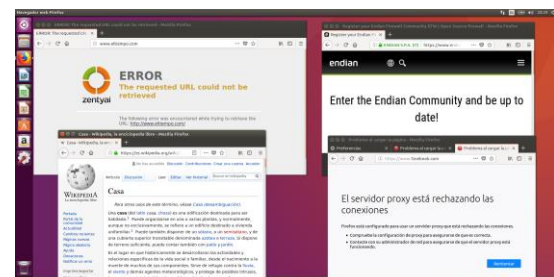


Fig. 28 Validación de Regla de acceso zentyal

III. TEMÁTICA 3: CORTAFUEGOS O FIREWALL

A. *Funcionamiento de los Cortafuegos*

Los cortafuegos usualmente son utilizados con el propósito de bloquear y/o limitar el acceso hacia y/o desde redes privadas y redes públicas. Por lo tanto, es posible usarlos para denegar o bloquear el acceso a algunos sitios de internet específicos.

Estos trabajan directamente sobre los protocolos de red y sobre IPs específicas permitiendo un grado de control bastante específico y profundo, pero a su vez agregando mucho trabajo a la hora de configurarlos y mantenerlos; principalmente porque los sitios de internet que normalmente se desean bloquear tienen un gran número de IPs asociadas (Zentyal, s.f).

B. Herramientas de Zentyal

El servidor Zentyal cuenta con una interfaz de administración web que permite a través de un navegador configurar todo lo necesario para gestionar los servicios ofrecidos en Zentyal. Además, Zentyal ofrece un concepto denominado “Objetos de Red” que permite agrupar conjuntos de direcciones IP para luego aplicar reglas de acceso y control de tráfico sobre estos para poder utilizarla, facilitando en cierta medida su posterior administración (Zentyal, s.f.)

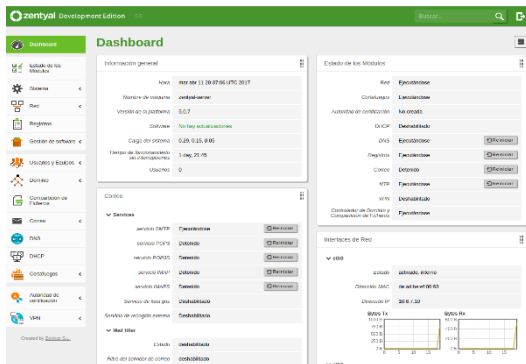


Fig. 29 Panel de administración de Zentyal

IV. TEMÁTICA 5: VPN

Las empresas por lo general tienen redes LAN y WLAN para las oficinas, pero en ocasiones se requiere que podamos ingresar a la red corporativa desde cualquier ubicación diferente a la infraestructura interna, es por ello que la utilización de servicios VPN (Redes virtuales Privadas) son altamente difundidos en entornos corporativos, el objetivo que se busca es que para el ordenador cliente no note si nos encontramos dentro o fuera de la organización y por ende las políticas de seguridad de nuestras aplicaciones aplican de manera normal.

El responsable de realizar esta tarea es el software VPN, funciona agregando una tarjeta de red nueva de manera que para el sistema es una tarjeta más que se comunicara con nuestro servidor que administra la conexión la cual consiste en:

- Autenticar un cliente: Se puede realizar a través de usuario y contraseña o con archivos de configuración o certificados de seguridad.
- Establecer un Túnel: a través de internet,

un túnel seguro que permite viajar los paquetes de red encapsulados desde la IP pública del proveedor de internet hasta nuestro servidor.

- Proteger el túnel: por ser una conexión a través de internet el servicio se encarga de encriptar la información para que no pueda ser extraída y utilizada por terceros.

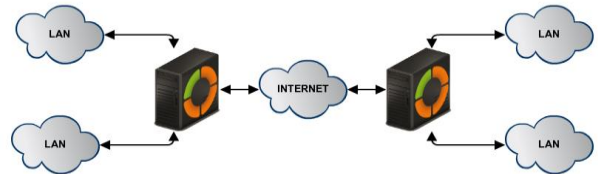


Fig. 30 Servidor Zentyal para salida a internet

En una arquitectura empresarial podemos observar como el comercial y el cliente se pueden comunicar con nuestra red usando internet y el servidor de Zentyal

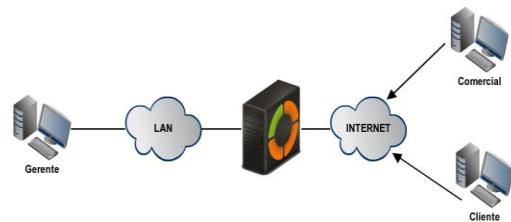


Fig. 31 Interconexión de varias redes LAN

También podemos interconectar varias redes Lan, usamos dos servidores VPN y internet como enlace.

Las VPN son importantes en los entornos corporativos por la movilidad que ofrece a los empleados y también por qué puede generar ahorros en costos importantes porque podemos utilizar internet como medio de enlace y no necesariamente tener enlaces dedicados que pueden encarecer la operación (Zentyal, s.f.)

Algunas de las desventajas que se puede identificar en las VPN es que por el cifrado y descifrado y por usar una red que redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos (Suarez, 2016b)

IX. CONCLUSIONES

Zentyal (Development Edition) es una alternativa a la herramienta informática funcional en entornos profesionales de diverso índole, y con gran alcance y posibilidades para pequeñas, medianas y grandes empresas que requieran de la protección y seguridad de su información, comunicación y manejo de la misma, favoreciendo una mayor accesibilidad por mantener unos costos más bajos que en otros programas con características similares, además que no requerir de unos equipos tecnológicos con características muy específicas sino que puede desarrollarse con un equipo con un hardware similar a computador personal, de tal forma que garantiza un buen rendimiento con su software seguro.

Por otra, esta tecnología se puede funcionar con diferentes servidores instalados en una red, logrado así una incorporación fácil mitigando costos en una implementación o fusión de tecnología.

REFERENCIAS BIBLIOGRAFICAS

Arias, P (2011). Diseño de una red LAN/WAN Seguridad para el Tribunal Constitucional aplicando la metodología de tres capas de CISCO. Consultado el 25 de mayo de 2018 de la web:
<http://repositorio.puce.edu.ec/bitstream/handle/22000/6371/9.21.001541.pdf;sequence=4>

Linode, (sin fecha) Sistemas Operativos. Consultado el 25 de mayo de 2018 de la web: https://www.goconqr.com/p/7868692-sistemas-operativos--mind_maps

Linode, (sin fecha) Tecnología LINUX, ERP Y Aplicación. Consultado el 25 de mayo de 2018 de la web:
https://issuu.com/elisaprada7/docs/revista_20_elisa_20m_20prada

Pedroza, P; Zuñiga, L; López, A; Mendoza, A & Arias, C (Sin fecha). Implementación De Servicios De Gestión De La Infraestructura Ti En Zentyal 5.0. Consultado el 23 de mayo de 2018 de la web:
<http://stadium.unad.edu.co/preview/UNAD.ph>

p?url=/bitstream/10596/14539/1/1130606405.pdf

Delgado, D; Jorquera, C; Sepúlveda, G & Zamora, C (2014). Redes de Computadores I Redes Privadas Virtuales (VPN). Consultado el 24 de mayo de 2018 de la web:
[http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20\(VPN\).pdf](http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20(VPN).pdf)

Nuami (sin fecha). ¿Qué son los cortafuegos? Consultado el 22 de mayo de 2018 de la web: <http://nuami.net/que-son-los-cortafuegos/>

Suarez, J (2016a). Servidor DHCP. Consultado el 22 de mayo de 2018 de la web: <http://www.juanluramirez.com/servidor-dhcp/>

Suarez, J (2016b). Servidor VPN. Consultado el 22 de mayo de 2018 de la web:
<http://www.juanluramirez.com/servidor-dhcp/>

Zentyal (Sin fecha). Zentyal, El Servidor Linux para pymes. Consultado el 22 de mayo de 2018 de la web:
<http://www.zentyal.com/es/zentyal-server/>